



IT万屋の役立つ話

ISM講座
18th October 2005

山本 学
Exlayer Limited

19/10/2005

www.exlayer.co.uk

生産性が上がる話

- ITを導入すれば、生産性が上がる訳ではない
 - (高いゴルフクラブやボールを購入しても、スコアーは。。。)
- 日常業務の流れを分析し、IT化のポイントを絞る
 - 業務フローの把握が必要
 - ITツール駆使するための仕組みやアイデアが必要
- ネットワークスキャナーが大活躍!!
 - これなしでは当社業務は成り立たない
- ペーパレス化の副産物は意外なところに
 - コピー機で3年間で使用した枚数が50枚以下
- ISO9001/品質管理、BS7799/情報セキュリティ管理を導入
 - Plan – Do –Check –Action の定着

19/10/2005

www.exlayer.co.uk



お客様に怒られない話

- お客様の要望はスピードと品質
 - 提案書や見積りが速い
 - システム導入／障害対応が早い
 - 品揃えが豊富
 - 品質が高い（技術力）
 - 品質が一定（誰でも対応してくれる／脱属人化）
 - **何とかしてくれる(総合力)**
- 要望に応じていくための取組み
 - 仕事のシステム化
 - 情報共有の強化
 - お客様の各種情報の履歴管理
 - 製品リサーチと評価
 - 満足度調査実施
 - Managerは8時入社
 - 社内教育

19/10/2005

www.exlayer.co.uk



情報共有の話

- ドキュメント管理
 - サーバのフォルダの構成をルール化して、同じ文章が点在しないようにする
 - InvoiceやDelivery NotesはPDFにしたあと、“YYYYMMDD Supplier”のようにネーミングする
- メール情報の共有
 - メールサーバ上に共有フォルダを作成して業務関連メールを保管
- 名刺管理
 - CardScanを利用（サーバ上にデータを保管し共有）
 - 検索が容易
 - LAPTOPで持ち出す（セキュリティ対策が必要）
 - 個人情報保護にも役立つ
 - IP電話と連携

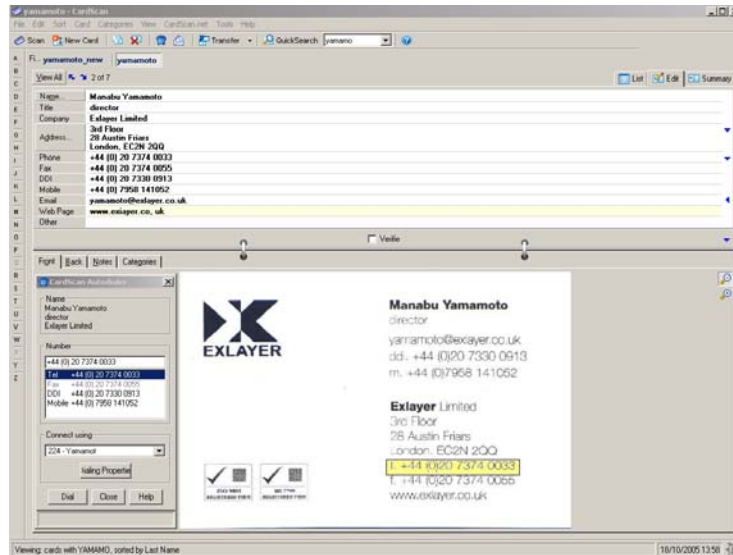
関連URL

<http://www.cardscan.com/home/index.asp>

19/10/2005

www.exlayer.co.uk

CardScan とIP電話の連携



19/10/2005

www.exlayer.co.uk

電子メールの話(その1)

- メールの秘話性
 - ハガキと同様で、誰でも読める。封筒に入った手紙の方が安全
 - 通信の内容は丸見え
- メールの信頼性
 - なりませんが簡単、筆跡鑑定できないのでハガキよりたちが悪い
- メールの信頼性が低いためにスパムメールやフィッシングメールが横行
 - 広告宣伝を無差別に送信
 - ワームによる送信
 - Phishing メールも増加一方(簡単に作れるパッケージ/ Bot net)
- 出張先からメールが送信できない
 - サーバ不正利用を防止する為に、送信元を制限している為

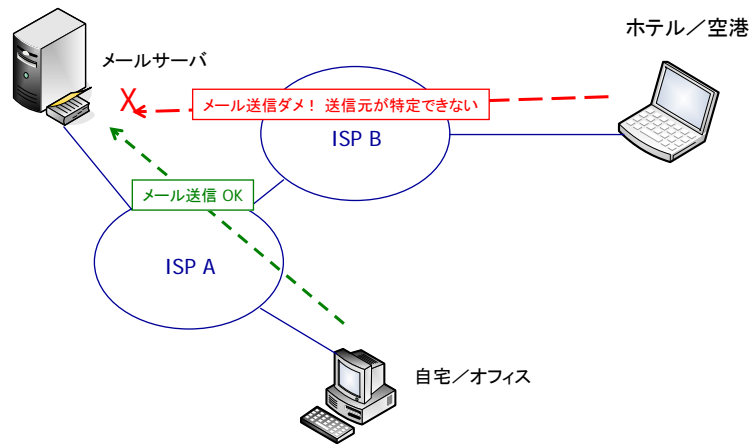
関連URL

<http://www.antiphishing.org/index.html>

19/10/2005

www.exlayer.co.uk

出張先でメールが送れない



19/10/2005

www.exlayer.co.uk

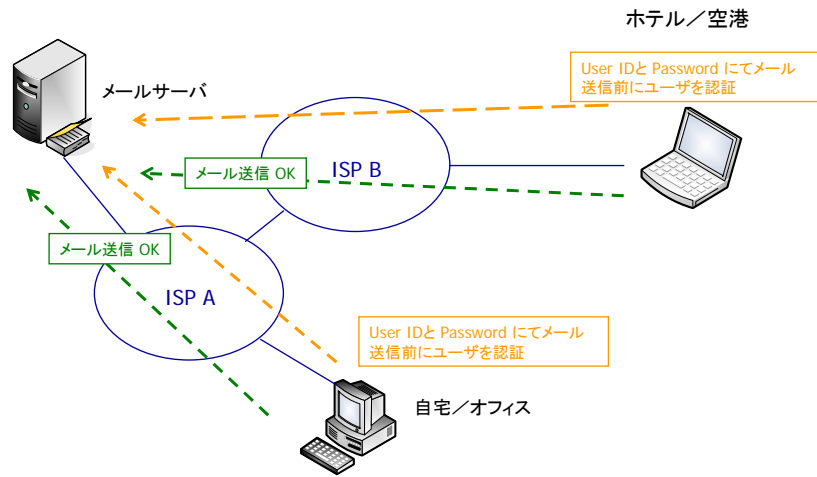
電子メールの話(その2)

- メールの特信性を確立するには
 - SSLによる暗号化を利用(社内メールが対象となる)
 - メール本文の暗号化(詳細は別途解説)
- メールの特信性を確立するには
 - デジタル署名を利用した、送信者の認証(詳細の別途解説)
- SPAM, Phishing対策
 - メールサーバ間での認証(SenderIDやSPFが協議、話会まとまらない)
 - 企業向けにはアプライアンスがあり、自己学習タイプとデータベースマッチング方の二つがある。(9割以上は退治できる)
- 出張先からメールを送信するには
 - SMTP認証機能があれば、どこからでも送信できる(提供するISPもに増えてきている)

19/10/2005

www.exlayer.co.uk

SMTP認証によるメールの送信



19/10/2005

www.exlayer.co.uk

SpamやPhishingの増加要因

- 要因
 - ブロードバンド普及に伴いセキュリティ対策のとられていないPCの急増
 - ユーザへの危険性の通知が十分でない
 - ゾンビPC (Bot PC/ Bot net) が急増、組織だった犯罪
 - ユーザ知らないうちにスパムメールを送信
 - Webサイトへの攻撃に利用される
 - 各種ツールが簡単に入手できる
- モチベーション
 - 昔は、自己顕示欲を満たすため
 - 最近では、単純にビジネス目的(金銭)に移ってきており、組織的な犯罪が増加

関連URL

http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf

19/10/2005

www.exlayer.co.uk

分かり易い暗号化の話

- 公開鍵暗号化基盤 (PKI)
 - 対になる二つの鍵を生成 (ペリサインなどが鍵の管理と身元保証を供する)
 - 秘密鍵と公開鍵
 - 秘密鍵は個人で厳重に保管が必要
 - 公開鍵は他人に広く公開する (ペリサインのサイトで検索可能)

関連URL

- <https://digitalid.verisign.com/>

19/10/2005

www.exlayer.co.uk

公開鍵の入手

(<https://digitalid.verisign.com/services/client/index.html>)

VeriSign Digital ID Services

Home Help with this Page

Search For Digital IDs

Search our online database for anyone's Digital ID by entering the name, e-mail address, or serial number and issuer name contained in the Digital ID, and clicking on the SEARCH button. If you cannot locate a Digital ID by e-mail address or name, the owner of the Digital ID may have chosen to "unlist" it when setting Digital ID preferences. In order to find it, you will need to obtain the serial number and issuer name of the Digital ID from its owner.

You cannot use wildcard characters. By clicking the SEARCH button you accept the terms of our [Relying Party Agreement](#).

Search by E-mail Address (recommended):

Enter the E-mail Address:
(example: john_doe@verisign.com)

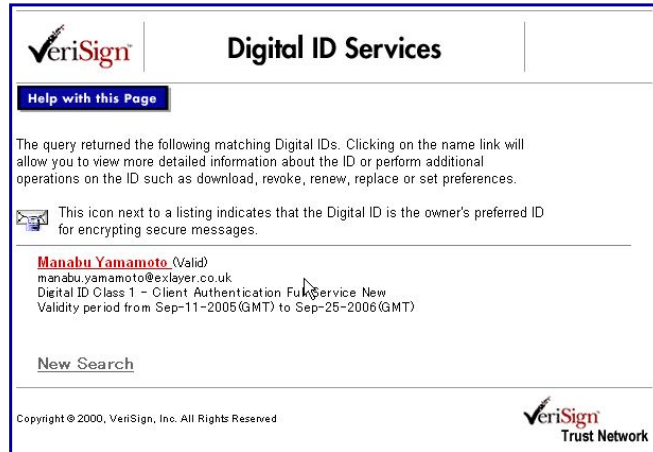
Search for Digital IDs that are:

Valid Expired All
 Revoked Pending

19/10/2005

www.exlayer.co.uk

公開鍵の入手 (検索結果)



The screenshot shows the VeriSign Digital ID Services search results page. At the top, there is the VeriSign logo and the title "Digital ID Services". Below this is a section titled "Help with this Page" which contains instructions on how to use the search results. A specific result is listed for "Manabu Yamamoto (Valid)" with details about the digital ID class and validity period. There is a "New Search" link at the bottom of the results section. The footer of the page includes the copyright notice "Copyright © 2000, VeriSign, Inc. All Rights Reserved" and the VeriSign Trust Network logo.

19/10/2005

www.exlayer.co.uk

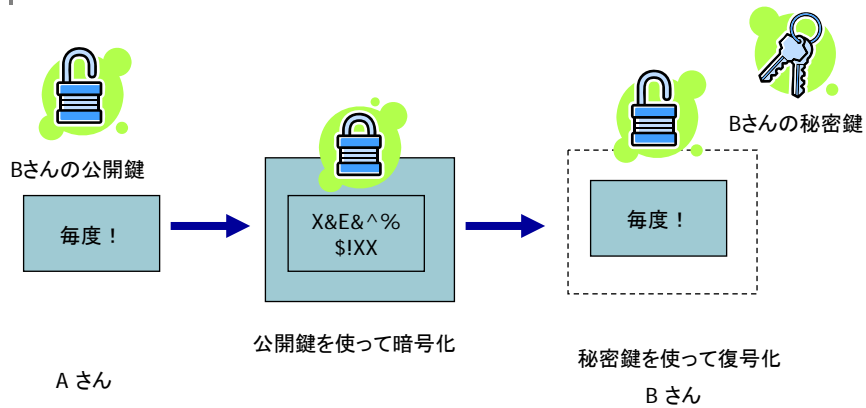
分かり易い暗号化の話

- メールの暗号化に利用(S/MIME)
 - ペリサインでデジタル署名を購入 年間20ドル程度 (秘密鍵と公開鍵)
 - 秘密鍵をPCにインストール (IE に取り込む)
 - メール送信相手の公開鍵を入手 (IEに取り込む)
 - メールの作成、送信相手の公開鍵で暗号化
 - 自分の秘密鍵で署名
 - メールを送信
 - 受信側では、自分の秘密鍵をIE に取り込み解読の準備をしておく
 - 送信者の公開鍵を入手 (IEに取り込む)
 - 暗号化されたメールを 自分の公開鍵で解読 (暗号化解読)
 - 相手の秘密鍵の署名を、相手の公開鍵で確認 (相手認証)

19/10/2005

www.exlayer.co.uk

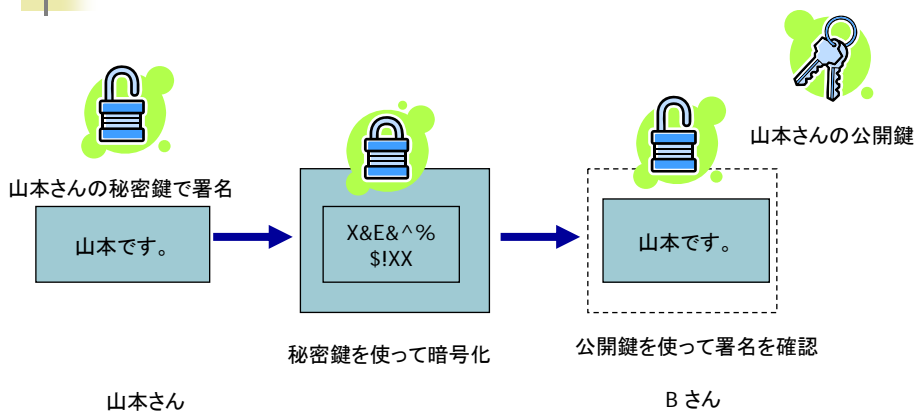
暗号化のイメージ



19/10/2005

www.exlayer.co.uk

署名のイメージ



19/10/2005

www.exlayer.co.uk



パスワード解読の話

- パスワードだけではセキュリティは確立できない
 - キャッシュカードは3回でロック
 - Windowsへのログオン(3回でロックすることを推奨)
- パスワード解読の実際
 - ツールがあれば誰でもできる(60ポンド)
 - 辞書攻撃、総当たり攻撃、
 - エクセルファイルの4桁パスワード解読は1秒以下
 - 長いほど解読時間は必要だが、100桁のパスワードでも総当たりで1週間程度あれば解読できる
- Windowsの管理者パスワードがリセットできる
 - FDD1枚、あるいはUSBメモリがあれば、Windows 管理者パスワードをリセットできる
- パスワードなしというセキュリティ設定
 - Windows XPではネットワーク共有へのアクセスはパスワードが必須

19/10/2005

www.exlayer.co.uk



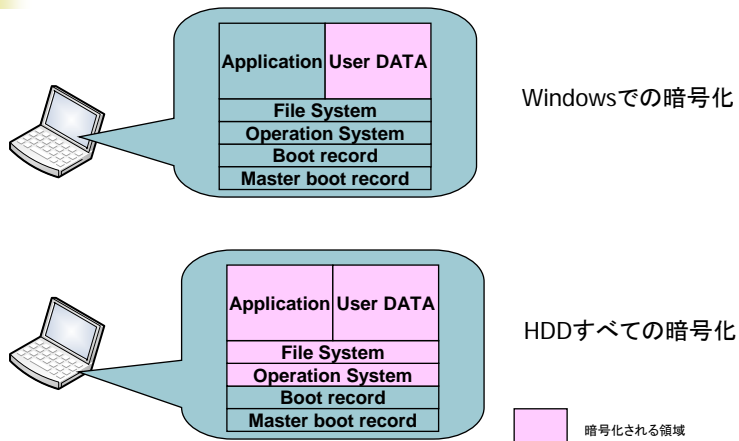
LAPTOP PCを守る話

- BIOSのパスワード
 - PCに標準で搭載される
- HDDの暗号化
 - サードパーティの製品を導入(safeboot)
- USB Key によるWindowsへのログオン
 - キャッシュカードとPIN番号組み合わせのイメージ
- WebサイトのIDとパスワードをUSB keyへ保管
 - PCにIDとパスワード残ることを防止
- 最近の動向
 - HDDを搭載しないPCが登場
 - エンジニアがPCなしでお客様宅へ訪問

19/10/2005

www.exlayer.co.uk

HDD 暗号化



19/10/2005

www.exlayer.co.uk

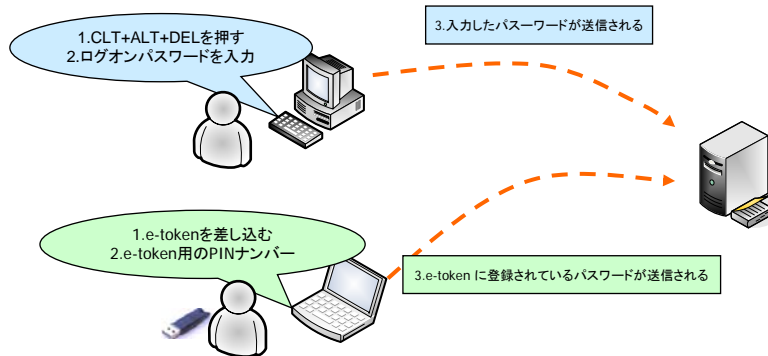
HDD 暗号化

- HDDを取り外し、別のシステムへ接続してもデータを読み取ることができない
- PC盗難/紛失時のデータ機密確保
- Windows パスワードのリセットにも対抗できる
- 万が一PCの盗難や紛失が発生しても、相当レベルの対策済みであることを公表できる(企業の社会的責任)

19/10/2005

www.exlayer.co.uk

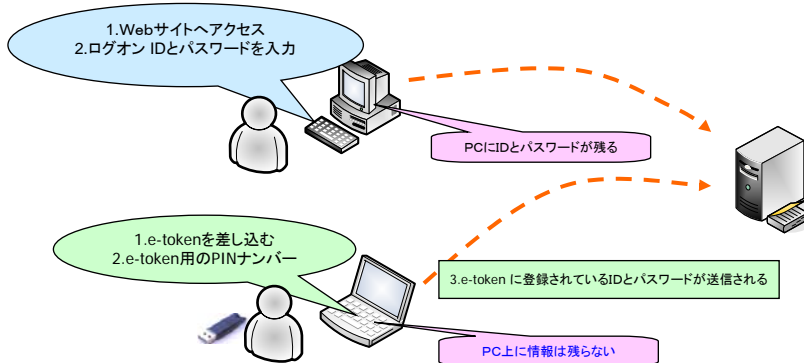
USB Key (Windows ログオン)



19/10/2005

www.exlayer.co.uk

USB Key (Web サインオン)



19/10/2005

www.exlayer.co.uk



USB key 導入効果

- Two-Factor 認証によるセキュリティ向上
- パスワードを複雑にするのが容易
- ユーザはPINコードのみ覚えておくだけでよい
- キーロガーによるパスワード漏洩対策
- PC上にID及びパスワードを残さない

具体的な用途

- オンラインバンキング用PCのセキュリティ強化
- イン트라ネットアクセス時のセキュリティ強化
- ラップトップPCの盗難対策

19/10/2005

www.exlayer.co.uk



インターネットVPNの話 (IPsec)

- IPsecによるインターネットVPNの普及
 - ブロードバンドの低価格化
 - 専用線からの乗り換えるケースも増えている
 - インターネットVPNがメインで専用線がバックアップ
- セキュリティは確保されているか？
 - セキュリティ強度と信頼性は非常に高い(暗号化技術を駆使)
 - 暗号化するための鍵の生成/管理をIKE(Internet Key Exchangeの略)と言う手順で行う
 - さらに用心深くIKEの通信自体もDiffie-Hellmanと呼ばれる共通鍵交換方式で、第三者に盗聴されることなく行われる
 - 万が一、鍵の情報が解読されたとしても、IKEは定期的(短い間隔)に鍵の再生成を実施することで、盗聴によるデータの暗号化解読の危険を最小限に留めることができる。新しい鍵が生成されれば、暗号解読は一からやり直しとなる。

19/10/2005

www.exlayer.co.uk

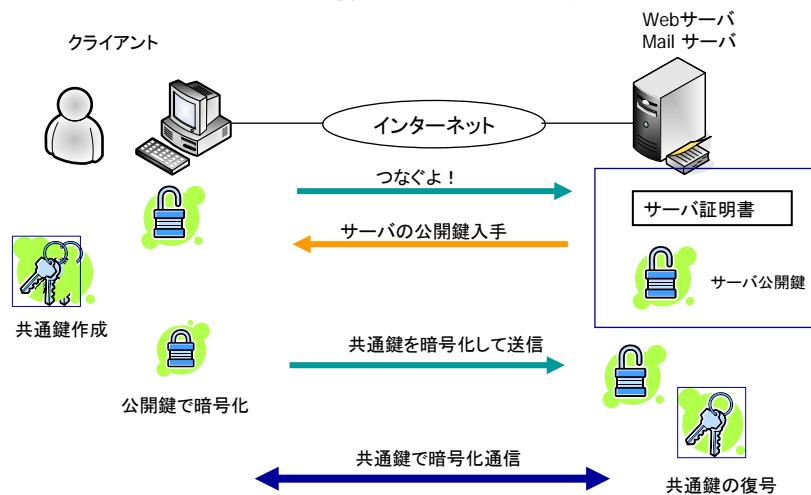
インターネットVPNの話(SSL-VPN)

- IPsecのリモートアクセスが苦手という問題点を解消
 - クライアントソフトの導入が不要(クライアントレス)
 - ユーザサポートの軽減
 - HTTPSが利用可能な環境であれば接続可能
 - 豊富なアプリケーション対応
 - Note, Outlookサポート
 - ターミナルサーバ
 - Webベースでのファイルサーバへのアクセス
 - PCの遠隔コントロール
- 具体的な活用
 - 営業先からの社内ファイルサーバへのアクセス
 - IT担当者の社外からの保守サポート

19/10/2005

www.exlayer.co.uk

SSL技術の概要



19/10/2005

www.exlayer.co.uk

TV会議システムの話

- そもそもISDN回線(128kbps)のキラーアプリとして開発される
- 1990年頃から登場、当時は1システムが数千万円と高額のため普及せず。
- 1998年頃から普及期を向かえる、価格も150-300万円に低下
 - しかし通信費用が高いため伸び悩む結果となる
- IP対応、やマルチポイント接続機能などを搭載
- 2003年以降は成熟期に入る。現在静かなるブーム(価格75万-150万円)
- このブームは、インターネットのブロードバンド化と、社内ネットワークの高速IP化が後押ししている
- インターネットや社内ネットワーク経由で通信すれば、実質通信費は無料
- 128kbpsのISDN回線利用時は日本向1時間 250ポンド (BT 4. 2ポンド/分)

19/10/2005

www.exlayer.co.uk

TV会議システム



19/10/2005

www.exlayer.co.uk

TomTom GO700



19/10/2005

www.exlayer.co.uk



GPS(TomTom)の話

- GPS2000年5月より、衛星の精度の制限がなくなり、従来の100-200mから10-20m以内となった。
- 測定の仕組み、3つ以上の衛星から電波を受信する必要がある。
- 衛星からの電波には正確な時刻と衛星の位置が含まれ、受信側で衛星からの正確な距離が分かるようになっている
- 欧州全土の地図内蔵
- Post Code およびStreet Name で行き先を指定
- Bluetooth で携帯と接続できハンズフリーホンになる
- HDD2GB内蔵
- POI(Point of Interest)
 - ガソリンスタンド、ホテル、娯楽施設、スピードカメラの位置など。。
 - インターネットから入手可能
- 民間衛星 IKONOS(イコノス)とGPSがあれば地球上に隠れる場所はないのかも？

関連URL

<http://www.tomtom.com>

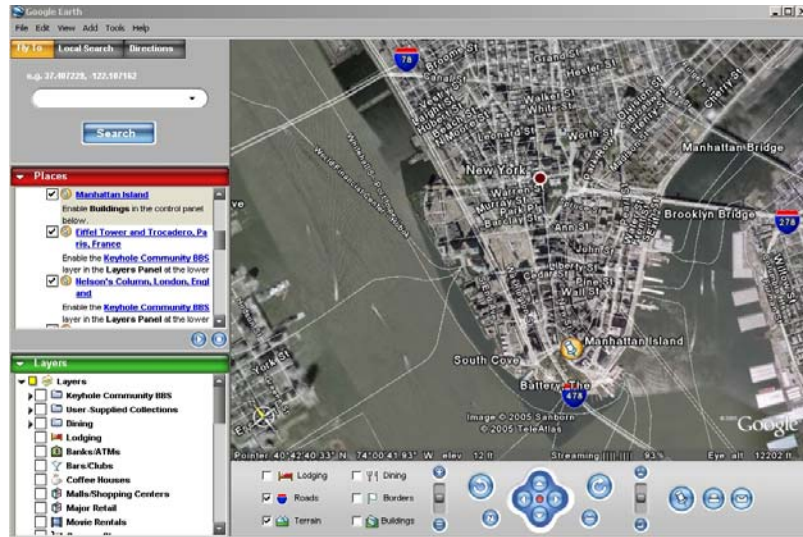
<http://www.pocketgps.co.uk>

<http://www.spaceimaging.com>

19/10/2005

www.exlayer.co.uk

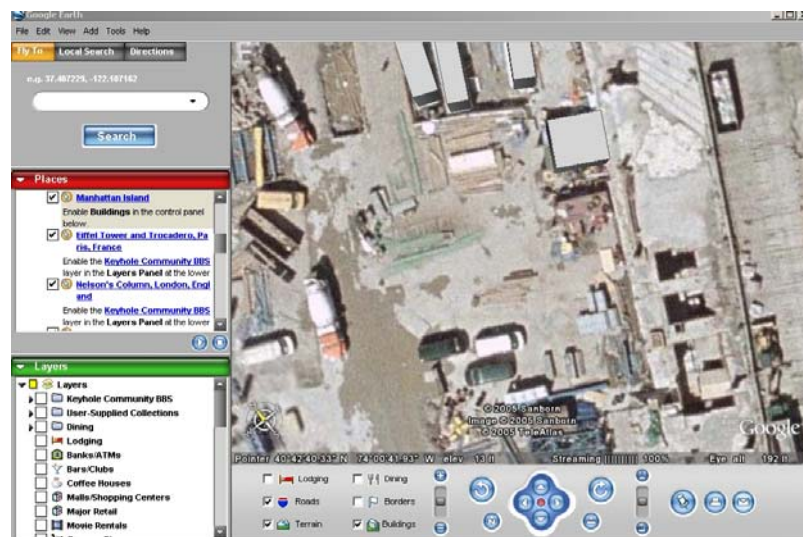
Google Earth



19/10/2005

www.exlayer.co.uk

Google Earth



19/10/2005

www.exlayer.co.uk